Unmasking Anonymous: An Eyewitness Account of a Hacktivist Attack

Tal Be'ery
Web Security Research Team Leader
Imperva

Agenda

- Anonymous Overview and Background
- How They Attack: Anatomy of an Anonymous Attack
  - Recruiting and Communications
  - Reconnaissance and Application Attack
  - DDoS
- Mitigations
  - What's hot - Mitigation Tools
  - What's not - Non-Mitigations Tools

2

Speaker Bio – Tal Be'ery

- Web Security Research Team Leader at Imperva
- Holds MSc & BSc degree in CS/EE from TAU
- Decade of experience in the IS domain
- Facebook "white hat"
- Speaker at Industry Events
  - RSA, blackhat, AusCERT
- CISSP

IMPERVA

Hacktivism - definition

"Hacktivism -
a portmanteau of *hack* and *activism*."

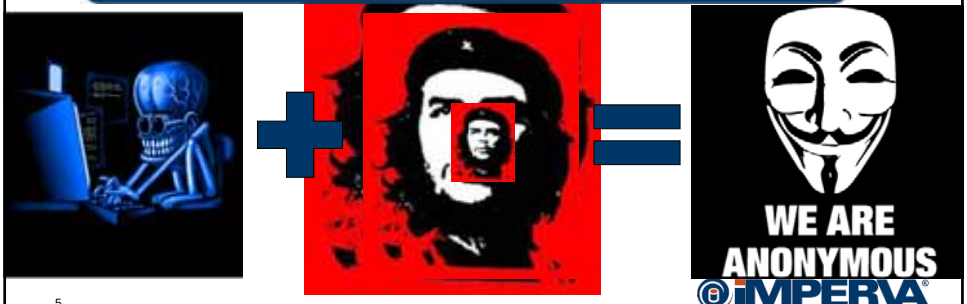
4

IMPERVA

What/Who is Anonymous?

"...the first Internet-based superconsciousness."
—Chris Landers. *Baltimore City Paper*, April 2, 2008

"Anonymous is an umbrella for anyone to hack anything for any reason."
—*New York Times*, 27 Feb 2012



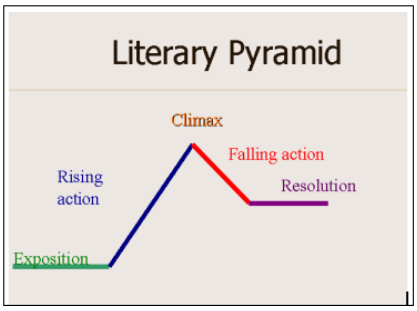
5

What/Who is Anonymous?

- One thing is for sure - they are hackers!

6

The Plot



- Attack took place in 2011 over a 25 day period.
- Anonymous was on a deadline to breach and disrupt a website, a proactive attempt at hacktivism.
- The website was mostly informational but contained data and enabled some commerce.
- The attack was not successful.

7

IMPERVA

On the Offense

+ **Skilled hackers –**
  - Small group , few individuals per campaign
  - have genuine hacking experience and are quite savvy.
+ **Nontechnical –**
  - can be quite large, ranging from a few dozens to a few hundred volunteers.
  - Directed by the skilled hackers
  - Providing rhe needed “muscles” to conduct DDoS attacks.

8

IMPERVA

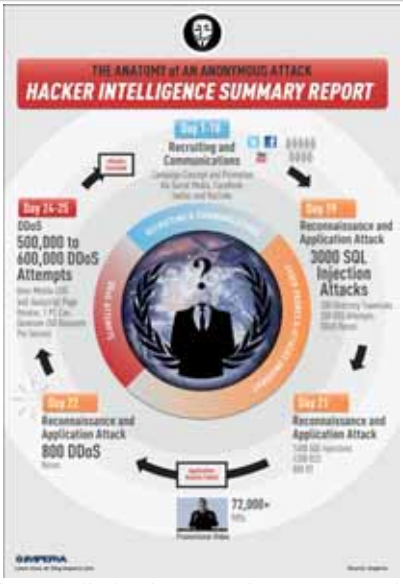
On the Defense

- Deployment line was network firewall and IDS, web application firewall (WAF), web servers and anti-virus.
- Imperva WAF
  - + SecureSphere WAF version 8.5 inline, high availability
  - + ThreatRadar reputation services
- Unnamed network firewall and IDS
- Unnamed anti-virus

9

IMPERVA

How They Attack: The Anonymous Attack Anatomy



10

for more: http://www.imperva.com/docs/HII_The_Anatomy_of_an_Anonymous_Attack.pdf

IMPERVA

1

Recruiting and Communications

Step 1A: An "Inspirational" Video

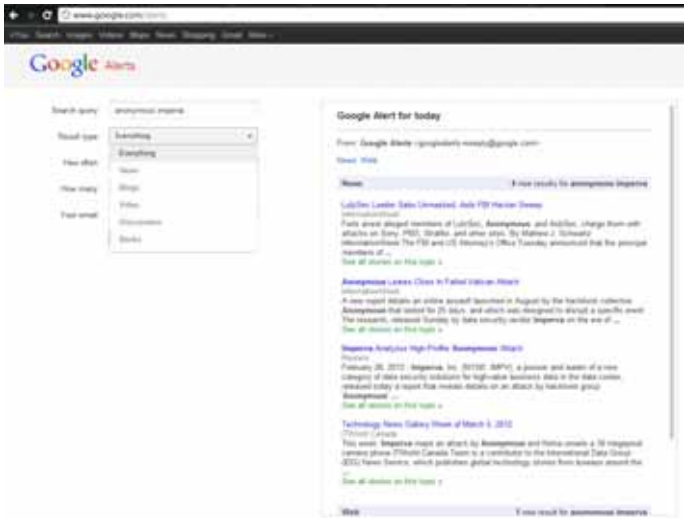
12

Step 1B: Social Media Helps Recruit

13

IMPERVA

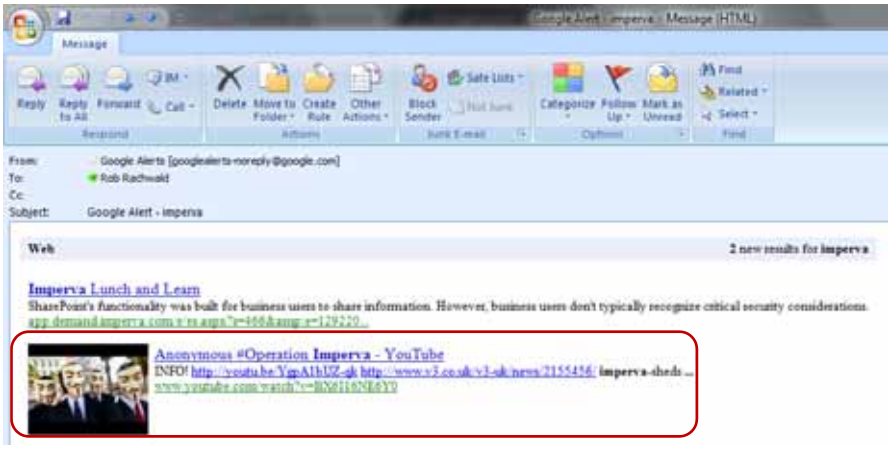
Setting Up An Early Warning System



14

IMPERVA

Example



15

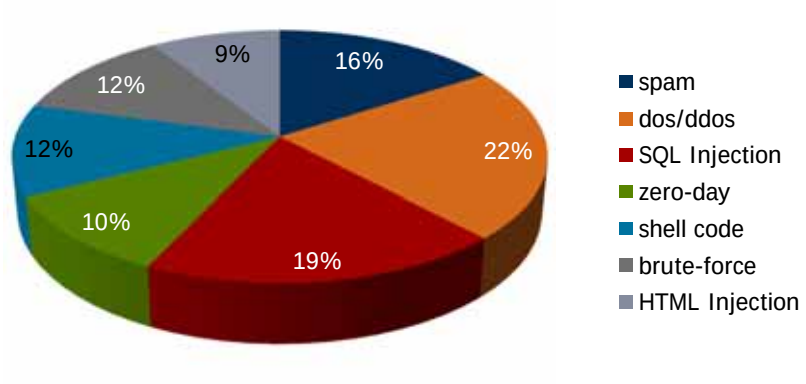
2

Recon and Application Attack

"Avoid strength, attack weakness: Striking where the enemy is most vulnerable."
—Sun Tzu

Anonymous' Attacks Mimic For-Profit Hackers

Hacker Forum Discussion Topics



Source: Imperva. Covers July 2010 -July 2011 across 600,000 discussions

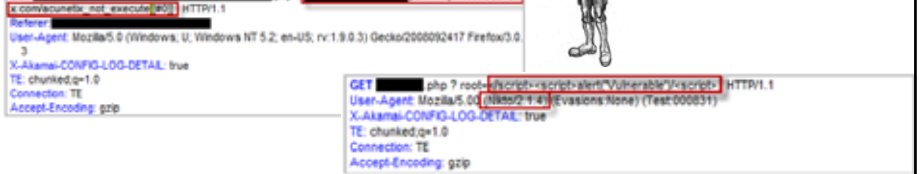
17

IMPERVA

Step 2A: Finding Vulnerabilities

- Tool #1: Vulnerability Scanners
- Purpose: Rapidly find application vulnerabilities.
- Cost: $0-$1000 per license.
- The specific tools:
  - Acunetix (named a "Visionary" in a Gartner 2011 MQ)
  - Nikto (open source)

acunetix

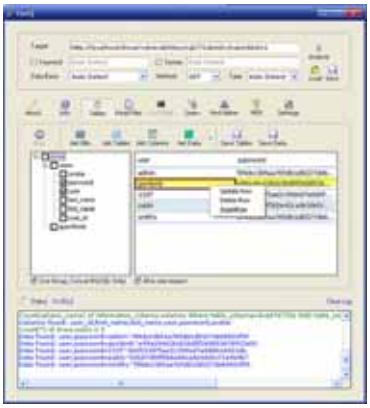


18

IMPERVA

Step 2B: Exploiting Vulnerabilities

- Tool #2: Havij
- Purpose:
  - + Automated SQL injection and data harvesting tool.
- Developed in Iran

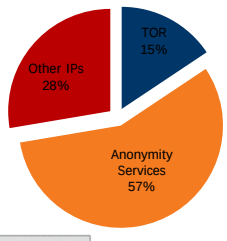


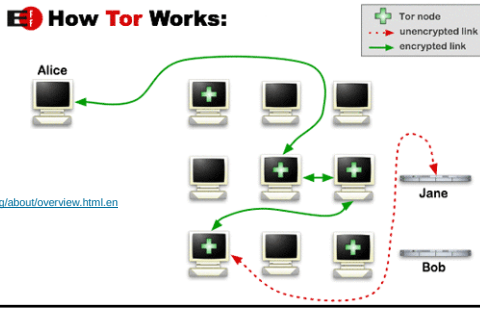
```
GET [redacted].php ? id=106147073' and ascii(substring((SELECT distinct table_name FROM information_schema.tables Where table_schema=0x202020 limit 0,1),2,1))=56 and 'x'='x  HTTP/1.1
Host: [redacted]
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; Havij
Connection: Close
```


IMPERVA

Protecting true Identity

- Hacker protect their identity
- By using
  - + TOR
  - + Other anonymity services
    - – Anonymous proxies
    - – Private VPN services
    - – Hacked servers





Source: https://www.torproject.org/about/overview.html.en

IMPERVA

Why hackers prefer using exploits over DDoS?

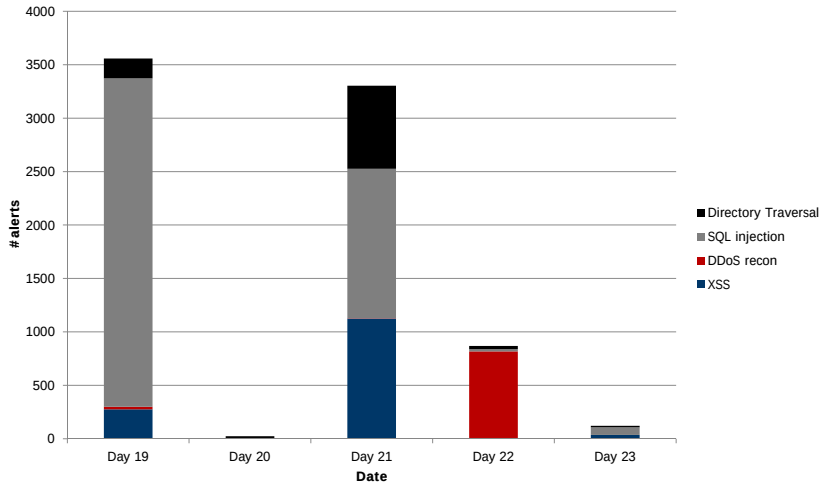
	Expoilts	DDoS
Damage	Inflict damage to all aspects of data security – availabili	Only data availability
Cost		n the site Hundreds, thousands..
Effect	Long lasting	Only during the attack

Exploits are the hackers first choice
DDoS is just a last resort

21

IMPERVA

Vulnerabilities of Interest



22

IMPERVA

Lulzsec hack Analysis #1- PBS

- SQL injection
- Exploited by Havij
- Defacement
- Administrative Data leakage

23

IMPERVA

Lulzsec hack Analysis #2- Militarysingles.com

- Executable file upload
- PII of 170K users leaked

24

IMPERVA

Mitigation: AppSec 101

- Dork Yourself
- Blacklisting
- WAF
- WAF + VA
- Stop Automated Attacks
- Code Fixing

25

iMPERVA

3

DDoS - the last refuge of a hacker

iMPERVA

Hacking Tools

- Low-Orbit Ion Canon (LOIC)
- Purpose - DDoS
- Windows desktop application, coded in C#
- UDP/TCP/HTTP flooding

IMPERVA

27

LOIC Facts

- LOIC downloads
  - 2011: 380K
  - 2012 (through April 22): 380K
  - Jan 2012 (megaupload takedown) =83% of 2011's downloads!

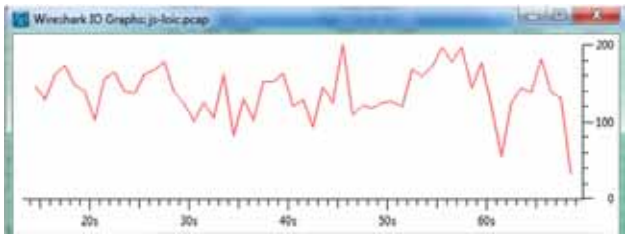
For more: http://blog.imperva.com/2012/05/loicversary.html

IMPERVA

28

Javascript/Mobile/VM/JS LOIC

- DaaS – DoS as a Service
- Easy to participate – no download
  - just point your browser to the JS-Loic page
- Application layer attacks
- Effective
  - Iterates up to 200 requests per second
- Cross platform
  - mobile device
  - Linux/Mac/PC



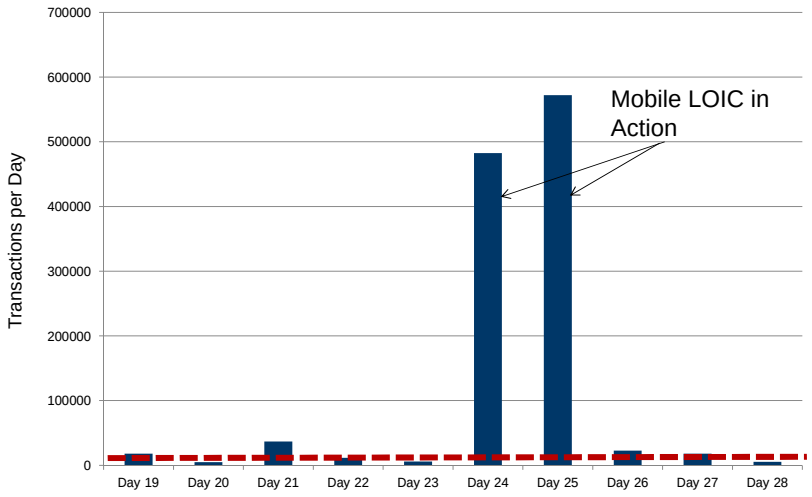
29

JS LOIC - Attack Characteristics

www.target.com/search.php?q=a&id=61278641278&msg=we+are+legion!

- Fixed target URL
  - Carefully selected to create load on target server
- A Parameter with some arbitrary changing value
  - To avoid caches along the way
- A Parameter value "msg" with some hacktivist's slogan
- HTTP Referer header – indicates attack code source

Anonymous and LOIC in Action



31

IMPERVA

DDoS Is Moving Up the Stack

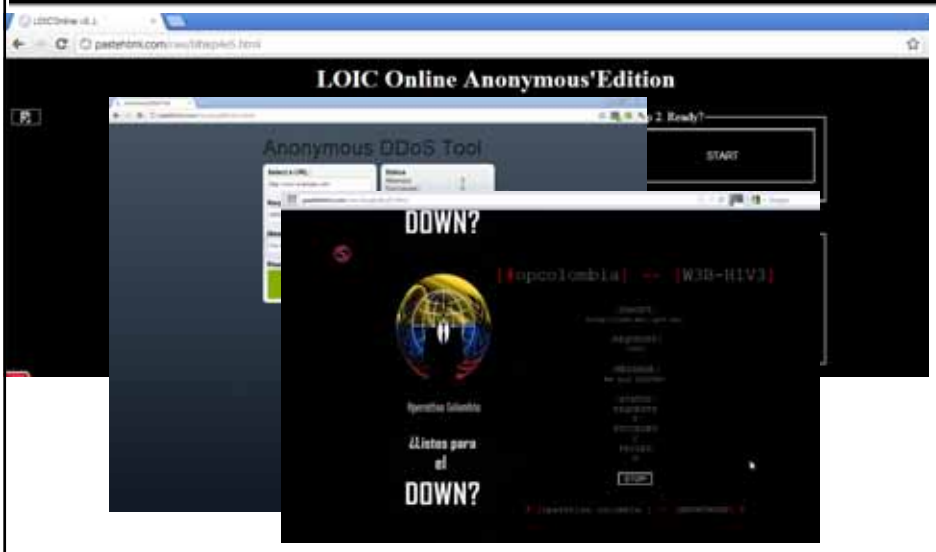
- Decreasing costs
  - + Application layer attacks are far more efficient
  - + Less attackers to take down a site
- The DoS security gap
  - + Traditionally, the defense against DDoS was based on dedicated devices operating at lower layers (TCP/IP).
    - – Don't decrypt SSL
    - – Don’t understand the HTTP protocol
    - – Unaware of the web application.

For more: http://blog.imperva.com/2011/12/top-cyber-security-trends-for-2012-7.html

32

IMPERVA

DDoS Is Moving Up the Stack



33

IMPERVA

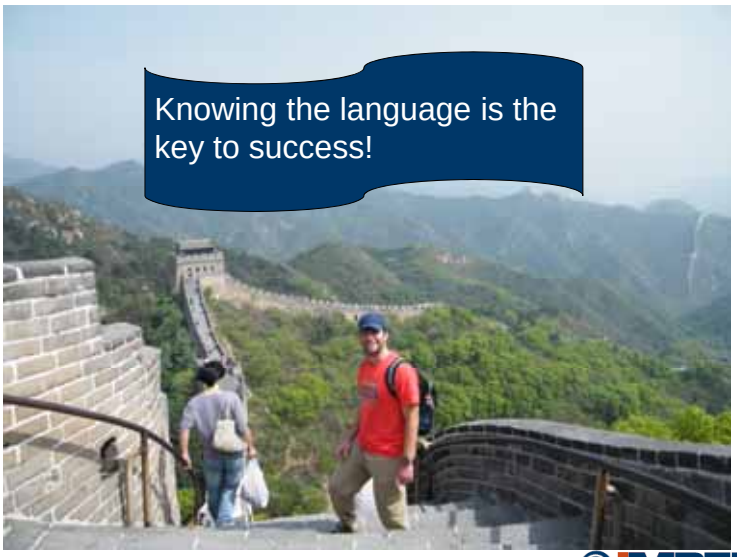
Mitigation

WAF: It can decrypt SSL, understand HTTP and also understand the application business logic to analyze the traffic, sifting out the DoS traffic.

34

IMPERVA

我不會說中文



35

IMPERVA

4

Non-Mitigations

IMPERVA

Anti-Virus is Irrelevant: Malware is NOT the MO

McAfee mea culpa

"The security industry may need to reconsider some of its fundamental assumptions, including 'Are we really protecting users and companies?'"

--McAfee, September 2011

Source: http://www.nytimes.com/external/readwriteweb/2011/08/23/23readwriteweb-mcafee-to-security-industry-are-we-really-p-70470.html?partner=rss&emc=rss

37

IMPERVA

I have IPS and NGFW, am I safe?

- IPS and NGFWs do not prevent web application attacks.
  - + Don't confuse "application aware marketing" with Web Application Security.
- WAFs at a minimum must include the following to protect web applications:

- Web-App Profile
- Web-App Signatures
- Web-App Protocol Security
- Web-App DDOS Security
- Web-App Cookie Protection
- Anonymous Proxy/TOR IP Security
- HTTPS (SSL) visibility

→ **Security Policy Correlation**

38

IMPERVA

I have IPS and NGFW, am I safe?

- IPS and NGFWs do not prevent web application attacks.
  - + Don't confuse "application aware marketing" with Web Application Security.
- However, IPS and NGFWs at best only partially support the items in Red:

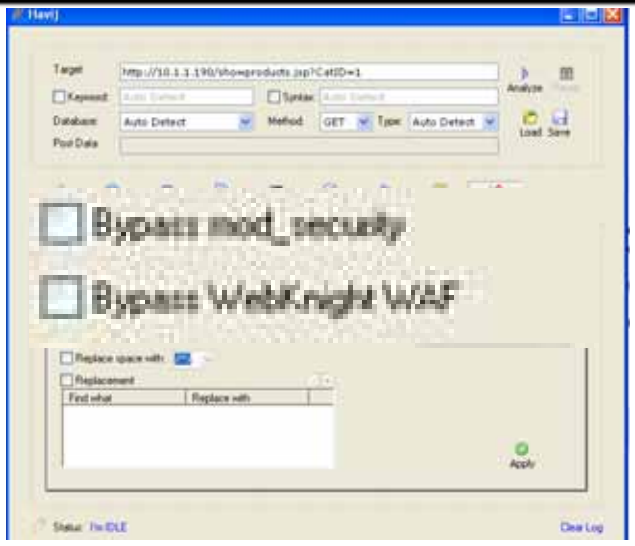
- ~~Web-App Profile~~
- **Web-App Signatures**
- ~~Web-App Protocol Security~~
- ~~Web-App DDOS Security~~
- ~~Web-App Cookie Protection~~
- ~~Anonymous Proxy/TOR IP Security~~
- **HTTPS (SSL) visibility**

~~**Security Policy Correlation**~~

39

IMPERVA

WAF is the solution - Hackers realize it too



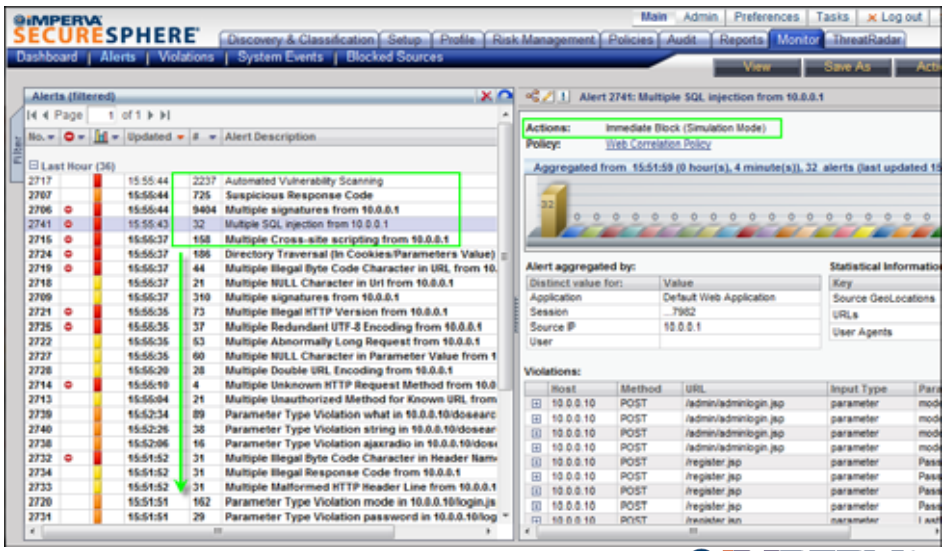
40

IMPERVA

5

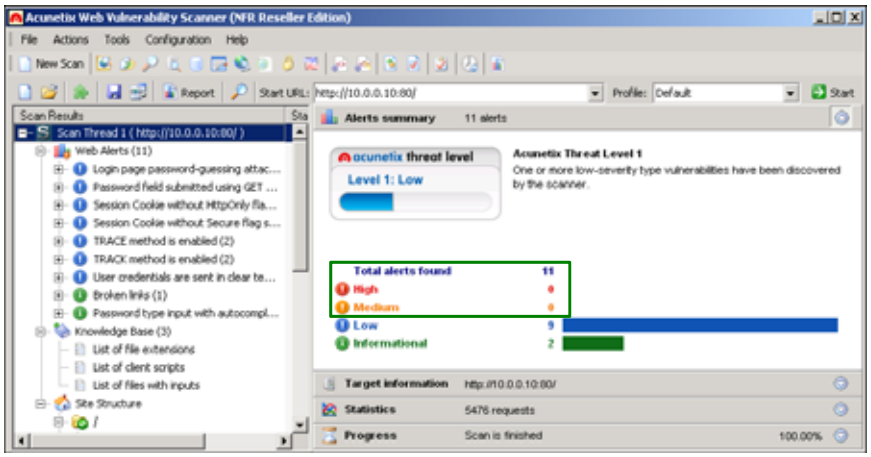
Mitigations

Automated Scanning Tools

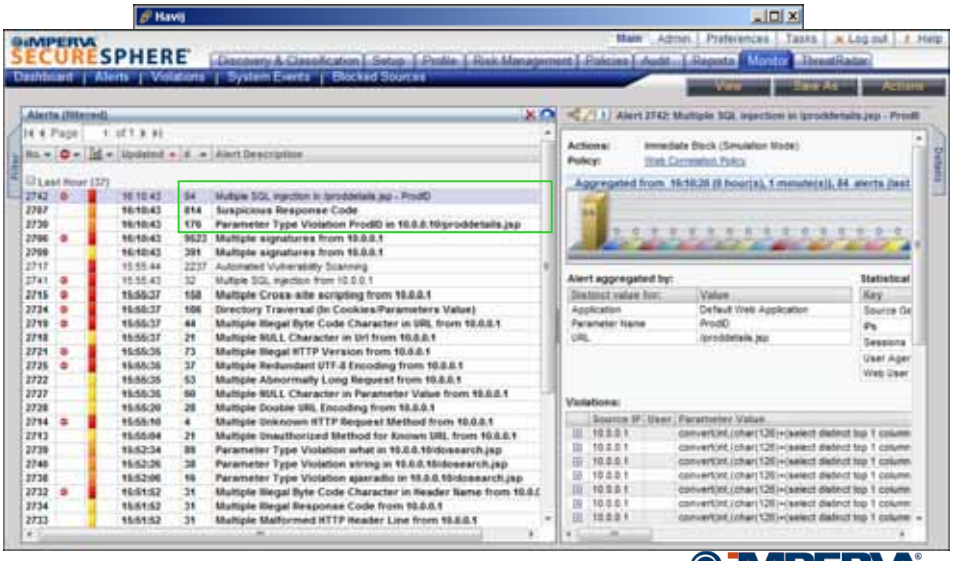


42

Automated Scanning Tools

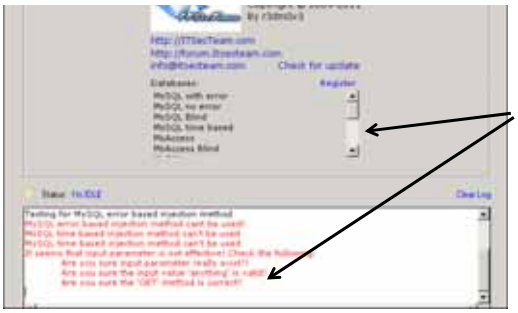


Automated SQL Tool



Automated SQL Tool

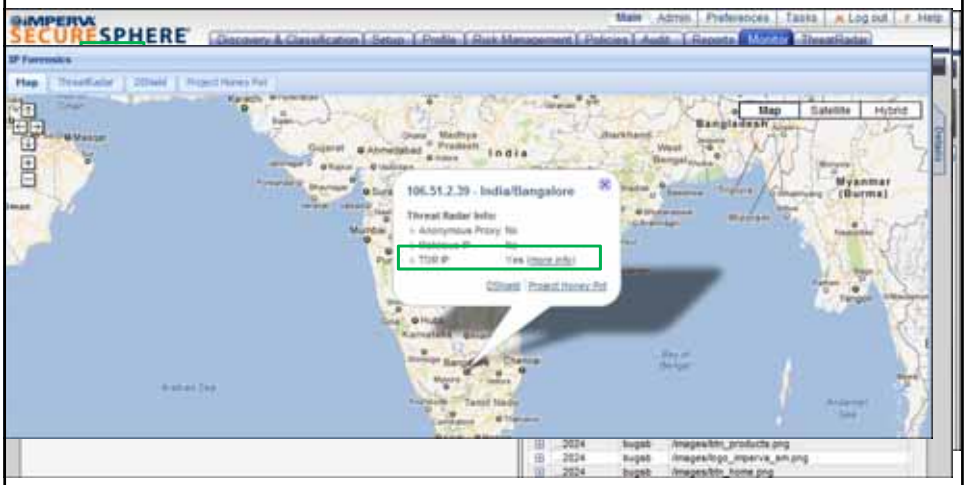
Testing for MySQL error based injection method
MySQL error based injection method cant be used!
MsSQL time based injection method can't be used
MySQL time based injection method can't be used
It seems that input parameter is not effective! Check the following:
Are you sure input parameter really exist?!
Are you sure the input value 'anything' is valid?
Are you sure the 'GET' method is correct?



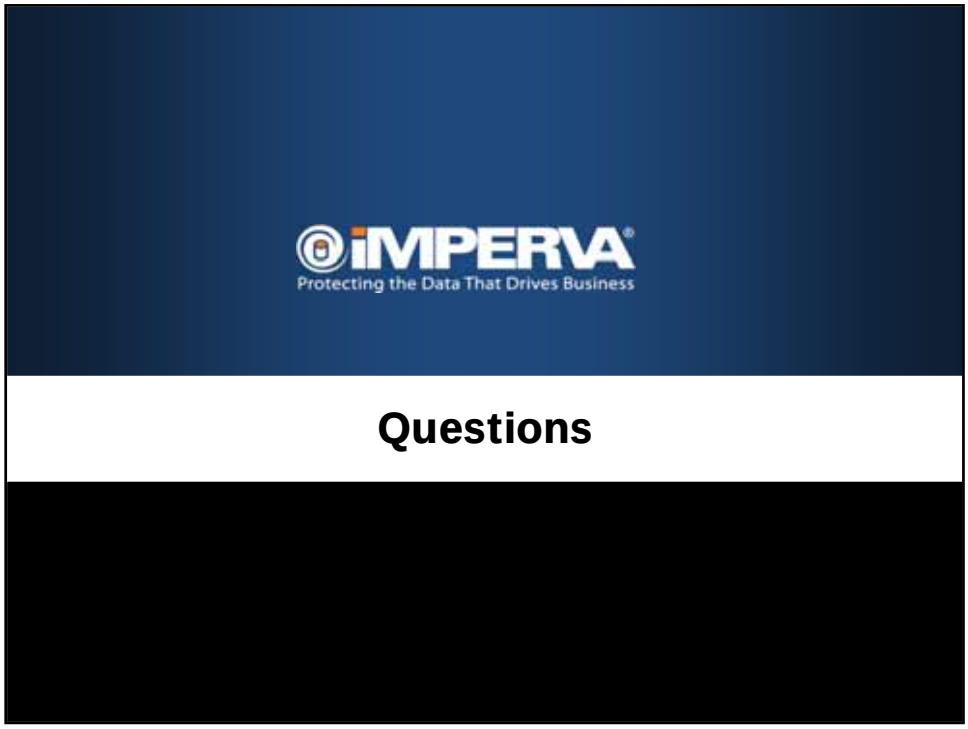
Havij SQL attack attempt fails with errors due to WAF mitigation.

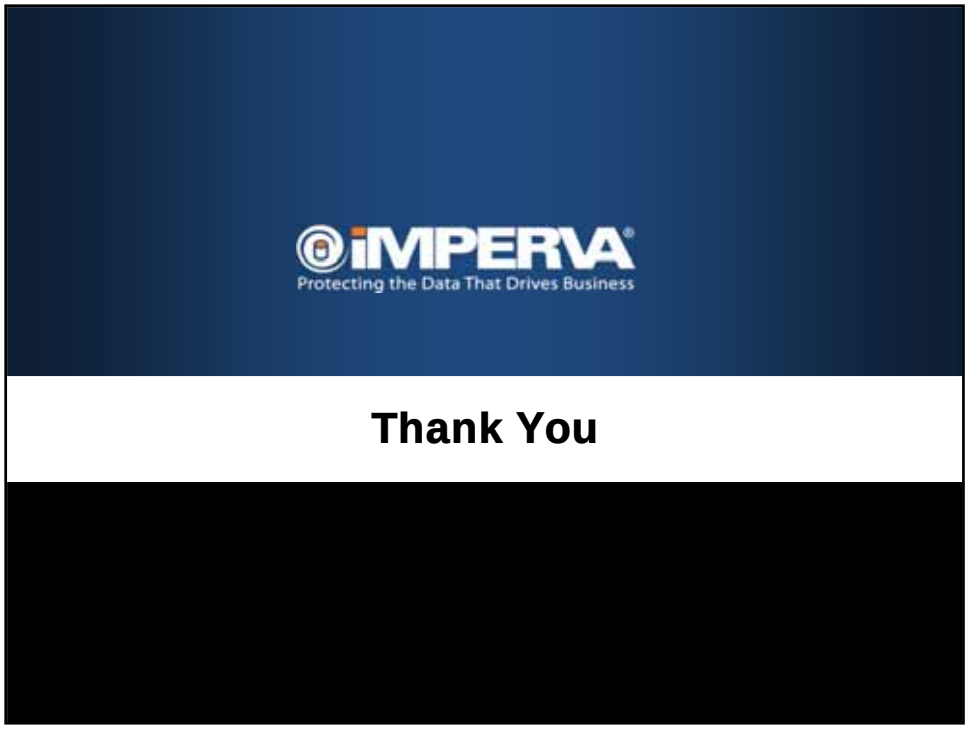
45

Blocking Traffic Based on Reputation



46


IMPERVA
Protecting the Data That Drives Business
Questions


IMPERVA
Protecting the Data That Drives Business
Thank You